情報理工学部　SN コース 3 回
アプリケーション脆弱性実習レポート

2600200443-6
Yamashita Kyohei
山下 恭平

May 30 2022

1　問 1

1.1　AchiverSample.zip の展開

AchiverSample.zip を脆弱アーカイブソフトを用いて展開したところ、特に異常なくデスクトップに展開することができた。その様子を以下の図 1,2 に示す。

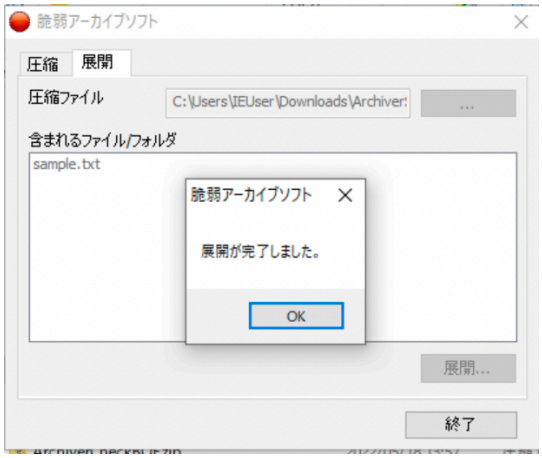

図 1

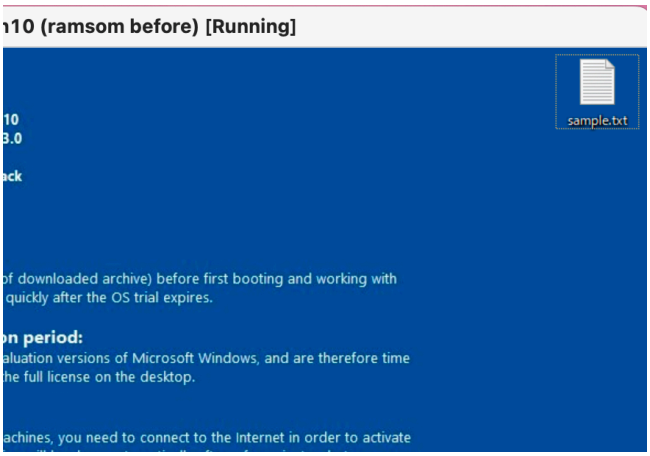

図 2

1.2　AchiverCheckBOF.zip の展開

AchiverCheckBOF.zip を脆弱アーカイブソフトを用いて展開したところ、ソフトが異常終了を起こし、展開できなかった。その様子を以下の図 3 に示す。

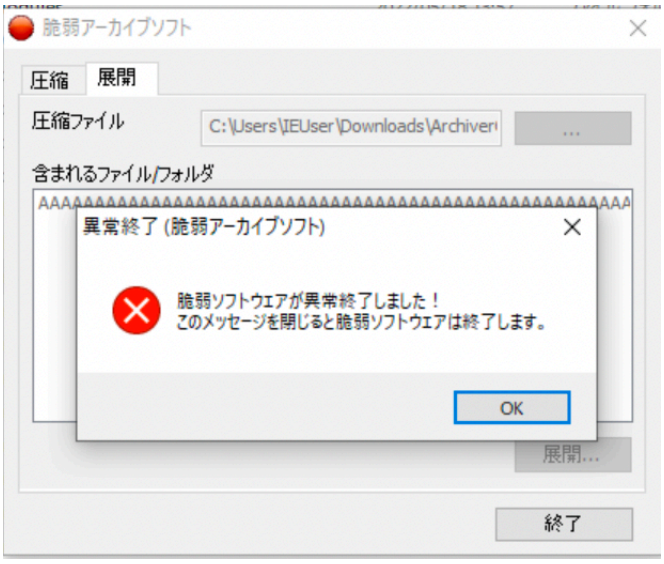

図 3

2　問 2

「AchiverAttackBOF.zip」を展開すると、「AchiverCheckBOF.zip」を展開した時と同様に、ダイアログが表示されて、プログラムが終了した。しかし、表示されるダイアログは、アプリケーションが強制終了されたことにより表示されたのではなく、オーバーフローにより、攻撃コードを埋め込まれたことにより表示されている。つまり、今回は展開するファイルにダイアログを表示するコードが埋め込まれていたことがわかる。次の図 4,5 にそれぞれのファイルを展開したときの様子を示す。

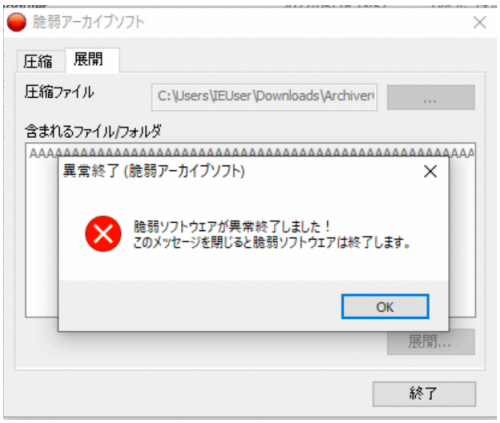

図 4　AchiverCheckBOF.zip

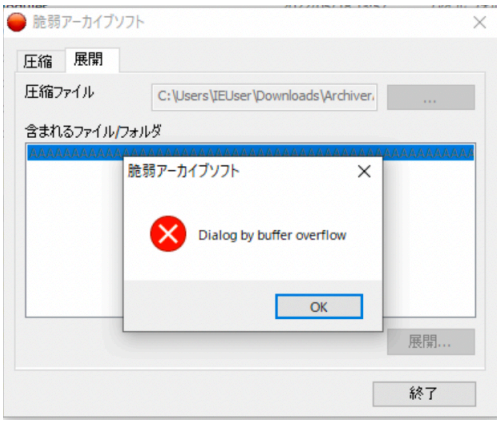

図 5　AchiverAttackBOF.zip

2.1　バッファオーバーフローが起きた際に起こる不具合の理由

プログラムの異常終了

オーバーフローにより、スタック領域に格納されている、呼び出される関数のアドレスや、関数からの戻りアドレスが書き換えられてしまうことで、プログラムが動作する上で、必要な関数等にアクセスできなくなるので、プログラムが異常終了する。
つまり、オーバフローを起こしても、元から格納されていたものと同一の内容で書き換えれば、プログラムは正常に動作すると考えられる。

プログラムの表示、変数値のバグ

オーバフローにより、元々設定されていた文字列などの情報も書き換えてしまうから。

2.2　スッタクオーバーフローを用いた攻撃方法と、その動作原理

オーバーフローにより、関数の戻りアドレスを書き換えることで、任意のアドレスにジャンプすることができる。この時、ジャンプ先のアドレスに対してもオーバーフローを利用し、任意の機械語を埋め込んでおくことで、攻撃者の意図した動作をさせることができる。

2.3　フォーマット文字列攻撃における「%n」の危険性

%n 書式は、その書式の直前の文字数を格納することができる書式である。
例えば、printf(”HELLO%n”, &n); と書き込むと n には 5 が格納される。よって、攻撃者は、任意の値をオーバーフローなどを起こさずに、書き込むことが可能である。さらに、「%(任意の数字)$n」と入力することで、スタック上の任意の位置を指定し、任意のコードを埋め込むことが可能である。

3　問 4

「AchiverCheckIOF.zip」を展開すると、プログラムが異常終了した。これは、脆弱アプリケーションが圧縮ファイルを展開する際の演算において、整数オーバーフローが発生し、プログラムが正常に動作しなくなったことで異常終了したと考えられる。次に、「AchiverAttackIOF.zip」を展開したところ、プログラムが停止したが、表示されるダイアログは脆弱アプリケーションのものとは別であることから、整数オーバーフローを利用して、攻撃者が埋め込んだコードが実行されたと考えられる。

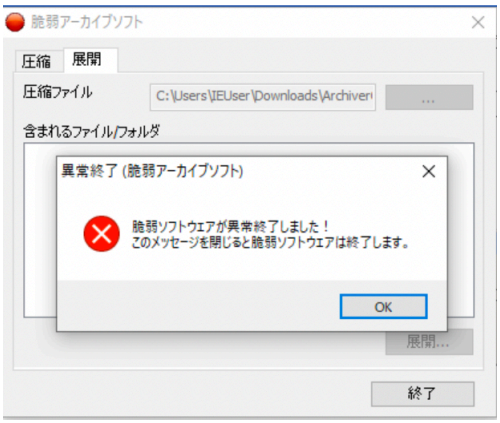

図 6　AchiverCheckIOF.zip

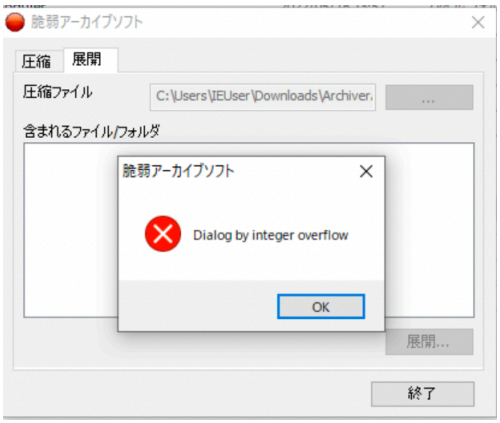

図 7　AchiverAttackIOF.zip